fraud. Materials ranging from press releases[47] to newsletters[48] to calling card materials[49] to formal brochures[50] have been described for (and sometimes provided to) the Commission. Information about customer seminars and training[51] and customer service aids available to customers on the matter of fraud prevention[52] have been described. The record demonstrates that, in the matter of customer education (including "warnings") there is nothing that needs to be mandated by the Commission.

It is obvious that carriers have sought to inform their customers about the perniciousness of telecommunications fraud, and to alert those customers to their own personal and financial responsibilities associated with such fraud.[53] Various "warnings" of various kinds are described in the submitted

---

[47]See, e.g., AT&T at Appendix A (middle part); Ameritech at 5.

[48]See, e.g., Ameritech at 2; Northern Telecom at 5.

[49]See, e.g., Bell Atlantic at 6; GTE at 17; U S WEST at 23-24 & Appendix C.

[50]See, e.g., Ameritech at 5; AT&T at 3 & Appendix A; Bell Atlantic at 6; GTE at 5 & Attachment A; MCI at 3; Northern Telecom at 4; Pacific at 6; U S WEST at 27-28 & Appendix B.

[51]See, e.g., BellSouth at 3; MCI at 3 & Attachment A; NYNEX at 4, 6; Northern Telecom at 3; U S WEST at 28-29.

[52]See, e.g., Ameritech at 2, 7; AT&T at 3, 9; MCI at 3-4; Northern Telecom at 4-5; Pacific at 6 & Exhibit B; Sprint at 3-4 & Attachment A.

[53]See, e.g., U S WEST at 45 & Appendix B at 2; GTE at Appendix A at 13; Pacific at 6, Appendix B at 8.

materials.[54] PBX customers are currently being provided with warnings -- both by manufacturers and CPE vendors. Payphone providers are increasingly knowledgeable about both the infirmities and strengths of CPE intelligence.[55]

While the Commission might feel compelled to institutionalize "warnings" associated with the sale of the CPE commodity, we see nothing in the record that would warrant "mandated" customer warnings about fraud and carrier services.[56] U S WEST opposes the suggestion of the PaPUC, and to some extent AT&T, that carriers (in particular LECs) be required to "warn" customers either annually or semi-annually about telecommunications fraud, in bill inserts or otherwise.[57] No credible record has been provided that would indicate such warnings are necessary; and the provision of such warnings would not be without considerable expense.

---

[54]See, e.g., U S WEST at Appendix B; Northern Telecom at 3-4.

[55]See, e.g., FPTA at 9.

[56]See MCI at 6 (no need to warn customers about carrier interconnecting services when it is CPE that is compromised in most fraud situations). Compare Himont at 1 (monthly billing insert); NATA at 15 (arguing that IXCs should have to provide warnings in monthly bills); ARINC at 2 (at the first bullet item on that page, ARINC outlines its warning scheme, but it is difficult to get a concrete idea of what its suggestions might actually require in action).

[57]See PaPUC at 4-5; AT&T at 4-5.

For example, there is little to no record comment with regard to fraud and the residential customer.[58] To the extent that fraudulent calling is associated with residential customers, it is primarily associated with calling cards. U S WEST already provides fraud prevention information to our residential customers when they receive a calling card. Additionally, other industry promotional materials advise how best to use a calling card to avoid fraudulent use. Little benefit would be accomplished by sending a bill insert to our mass market customer base.

Furthermore, a bill insert is not a vehicle that can be easily directed to discrete market segments or categorized by customer idiosyncracies. Thus, U S WEST could not use this vehicle easily to communicate just to business subscribers. Warnings directed to businesses would either have to be sent to all customers with an advisory that the message is directed to businesses only, or would have to be done via a separate mailing. A separate mailing is considerably more expensive than a bill insert.

Given the extensive record on the level of existing customer informational efforts with regard to telecommunications fraud, the Commission should not mandate anything additional. Carriers

---

[58]Compare AT&T at 6 (contending that customer CPE warnings should be limited to multi-line equipment capable of connecting incoming lines to outgoing lines).

are motivated to keep their customers' good will.[59] That means carriers are already motivated to help their customers in their attempts to avoid fraud in the first instance and to protect themselves against future fraud. A pre-published envelope-stuffing bill insert is not necessarily an effective means to accomplish this result.

U S WEST also vigorously disagrees with the suggestion of ICA that when customers initiate service they should be provided with a written warning about risks associated with network services; and that larger customers should have to provide a written acknowledgment of those risks, i.e., an assumption of the risk.[60] Such a requirement is totally unnecessary. Most customers are not damaged by "network fraud," and a general advisory that fraud can occur in the network would be no more meaningful than a general advisory that car accidents can occur on the highway. U S WEST already does considerable advisory work with our larger business customers, as we indicated in our opening comments.[61] Getting a "signed" document from these customers does not provide any added value to the existing process.

Carriers know their customers better than regulatory agencies. They know how to craft meaningful communicative

---

[59]See, e.g., AT&T at 12; GTE at 16-17; Pacific at 22; Sprint at 6.

[60]See ICA at 11.

[61]See U S WEST at 27-29.

materials and how to respond to demonstrated needs for information or services.[62] There is nothing in the record to suggest that carrier customer information campaigns were one-shot deals or were put into place to placate a regulatory agency bent on increasing carrier liability. The Commission should defer to the ongoing work of the carriers regarding customer information and awareness.

B. The Record Does Not Demonstrate that LECs Should Be Required to Develop/Deploy Additional Capabilities to Protect Against Fraud

A number of commentors argue that, insofar as fraud prevention is concerned, the LECs have -- inappropriately -- taken a back seat with regard to fraud prevention.[63] These commentors suggest that the Commission compel LECs to offer additional services, either by way of network monitoring[64] or

---

[62]See Sprint at 6; WilTel at 8.

[63]See, e.g., ACUTA at 2; APCC at 20-21; ISLUA at 2; NATA at 3; IPANY at i, 10-11, 13-14.

[64]The Commission needs to pay particular attention to the comments on monitoring services. While some commentors contend that "carriers" (including both LECs and IXCs) should be required to provide additional monitoring services in the network (see, e.g., API at iii, 12; ARINC at 2-3; ICA at 11; IPANY at Summary, 18; Kansas Turnpike Authority at 1; Metro-North at 2; MPA at 4; NJPA at 2; PaPUC at 5-6; SCOIR at 4; TCA at 5; User Parties at ii-iii), others (while using the term "carriers") appear to confine this obligation, either by specific reference or by context, to IXCs. See, e.g., APCC at 22-23; ICA at 11; NATA at 2, 3-END; TCA at 5; User Parties at 6 (but see at 8 n.16). Compare AT&T at 13.

additional blocking/screening services.[65] The Commission should decline this invitation.

1. Network Monitoring for Toll Fraud

The LECs' networks are not well suited to interstate or international telecommunications monitoring;[66] and to mandate that they become suited to such activities would be inefficient and could well be redundant. The larger IXCs have already established network monitoring services in their networks and it makes no sense to require LECs to duplicate such functionalities. As Sprint suggests, each network element need not have all possible fraud prevention capabilities, and it would create inefficient redundancies to require that they do.[67]

Networks should operate in a complementary fashion, however. An industry organization is the best place to assure that such complementary development for fraud prevention occurs over time.[68]

---

[65]See, e.g., IPANY at ii, 16.

[66]IPANY argues that LECs should be required to monitor COCOT lines. See IPANY at ii, 18 (arguing that "LECs, have the ability to monitor usage on telephone lines, on a real time basis[.]"). While New York Telephone might have this capability, U S WEST does not.

[67]See Sprint at 16, 19.

[68]See id. And see Section VI. below.

2. Access Restriction Services

While LECs' networks are not well suited to interstate and international toll monitoring, they have been utilized in the past to deploy access restriction and blocking services. As demonstrated by U S WEST's opening comments, U S WEST currently offers certain access restriction services, which customers employ to control network access -- not necessarily to protect against fraud. Those services include toll restrict (i.e., no toll calling at all), 976/900 access restrictions (i.e., no 976/900 calling at all), and so on.[69]

As the above service descriptions demonstrate, access restriction or blocking services are currently fairly binomial: access either is permitted or it is not. Such access restriction services are not now easily manipulated to accommodate ranges of customer choice. And, they do not precurse network capabilities associated with real-time interactive monitoring and the exercise of serendipitous customer choice.

In light of the above, two comments deserve particular attention. First, the suggestion by some commentors that LECs develop blocking capabilities to the 809 NPA.[70] Second, the suggestion that LECs develop access/blocking capabilities with

---

[69]See U S WEST at 17-19.

[70]See, e.g., APCC at iii, 19-20; IPANY at Summary, 16-17; FPTA at 12. International blocking capabilities do not block 809 access. 809 is an NPA recognized in the North American Numbering Plan as a domestic call, given the nature of the relationship between the United States and the termination locations (which are either territories or Commonwealths of the United States).

respect to certain or all NPAs/NXXs (or terminating numbers), allowing a customer to open or block access to calling destinations, at the customer's discretion.[71] Both suggestions are short on facts or implications that might educate a public policy determination.

Based on sound information,[72] U S WEST believes that fraudulent calling to the 809 NPA is overwhelming a regional problem (associated with East Coast calling). It would be most inappropriate to mandate certain calling or blocking configurations for the entire United States customer market based on an overwhelmingly geographically-isolated problem.

Furthermore, alternatives to mandated LEC blocking to the 809 NPA currently exist. Smart CPE (both PBXs and COCOT equipment) can be programmed to block access to 809 calling (and can often get even more discrete to blocking of 809/NXX traffic) using an exception list built into the equipment. In addition, certain carrier offerings apparently block access to the 809 NPA.[73] Based on these market conditions, it would be most

---

[71]See, e.g., O'Brien Engineering at 1 (customers should be able to control "country designations"); Stop & Shop at Attachment A, 1; User Parties at 5 ("customized call blocking functions"), 6.

[72]U S WEST secured this information from our representative to the Public Access Technical Forum ("PATF"), a forum dealing with national payphone technical issues.

[73]Compare, FPTA at 13 (noting that it has been advised that some IXCs have developed an international call blocking service that includes 809 for payphones presubscribed to that carrier).

inappropriate and inefficient to require LEC blocking of the 809 NPA.

The Commission should review those aspects of its various 900 dockets with regard to discrete NPA or SAC blocking.[74] Far from being a minor "inconvenience"[75] to establish, such blocking cannot currently be done in any economical or technologically feasible way.[76]

Only an entity that has never had to create a network "blocking" offering would assert that "a 'menu' of blocking options is both common and easily accomplished."[77] Nothing could be further from the truth.[78] Discrete number blocking

---

[74]See In the Matter of Policies and Rules Concerning Interstate 900 Telecommunications Services, Order on Reconsideration, 8 FCC Rcd. 2343 (1993) (particularly at 2349 ¶¶ 37-39) ("900 Reconsideration Order"); In the Matter of Policies and Rules Implementing the Telephone Disclosure and Dispute Resolution Act, Report and Order, 8 FCC Rcd. 6885 (1993) (particularly at 6895-96 ¶¶ 58, 63).

[75]See IPANY at 17.

[76]See U S WEST Communications, Inc. Opposition to American Telephone and Telegraph Company's Petition for Limited Reconsideration, CC Docket No. 91-65, filed Jan. 3, 1992, at 2-4 (discussing the concept of line class codes ("LCC") and LEC blocking) ("U S WEST Opposition").

[77]IPANY at 17, n.11.

[78]We remind the Commission that the public network was designed to be open -- not closed. Thus, every customer option associated with "closing off" access to the network requires some kind of gerrymandering -- usually involving combining desired blocked digits into some kind of common block. Also, as argued by Xiox at 2-3, there is a disturbing aspect to the "become more secure by becoming less open" approach to telecommunications fraud prevention. (While Xiox was focusing on CPE capabilities, the same can be said with regard to network access.)

> would be very costly for U S WEST to implement, and it would demand extensive switching capacity. Blocking is accomplished through the use of a[n] [LCC], which is given to each telephone subscriber. A separate LCC is required for each combination of the different categories of telephone numbers which can be blocked. As a result, the number of LCCs which are required increases geometrically with the number of categories. This means that while providing blocking for a single category . . . requires only one additional LCC, two categories would require three additional LCCs, three categories would require seven additional LCCs, and so on. [The formula is: the number of additional LCCs equals two raised to the power of the number of categories, minus one.] The proliferation of LCCs requires substantial resources, both to add to the capacity of switches, and to administer the provision of all of these additional blocking options to end users.[79]

An "809" block would be considerably difficult and expensive for LECs to implement. And, it might not even be possible in all central offices and with regard to all calls. The Commission should reject this "LEC-blocking" suggestion, in light of customer alternatives and the extensive cost associated with such a network solution.

The Commission should also reject those commentors arguing that the LEC network should be configured such that a customer can "customize" its access offerings, either those parts of the network that are open or those that are closed. The concept of a

---

[79]U S WEST Opposition at 3 & n.8 (shown in brackets in quoted text). Because of the problem associated with discrete blocking, for example, U S WEST currently blocks 976 and 900 services in a "common block." While it might be possible, despite the above problems, to "wrap" an 809 block into a common block, the Commission's earlier expressions on this matter indicate that it does not favor combining blocking of "information service" prefixes with other prefixes. See 900 Reconsideration Order, 8 FCC Rcd. at 2349 ¶ 39 (expressing concern over combining a 900 block with a 700 block).

closed network, open only at the customer's option, is fairly new and radical. In the future, as the LEC networks become far more intelligent, certain kinds of customer choice in this regard might well become available. But whether a customer will ever have total flexibility or choice with regard to network access remains to be seen.[80]

3. Screening Services

AT&T asserts that LEC blocking/screening services "were designed solely to prevent fraudulent calls[,]" and that it makes economic and public policy sense, then, for LECs to be responsible for the "failure[]" of these services.[81] AT&T is incorrect on both counts. First of all, U S WEST did not design its blocking/screening services "solely" to prevent fraud, but rather to aid customers in controlling access from their CPE into the network.[82] In some cases, this control prevents fraud; in other cases it prevents undesirable calling conduct from others on the premises, short of fraud. Furthermore, certain of these services (BNS, for example) is generally offered to our customers

---

[80]See, e.g., User Parties at 5 (who suggests that customers should be able to designate what prefixes they want opened and which closed. Presumably, a customer might want only one prefix opened (i.e., the one they call the most) and all others closed, with the option of opening prefixes at their discretion, if there appears a need. Compare arguments about Caller ID, that line blocking should be able to be "unblocked" at a caller's discretion.

[81]AT&T at 28-29. See also APCC at 6.

[82]See U S WEST at 16.

free of charge. It makes no economic sense, and even less public policy sense, to burden a free offering with the financial burden associated with completed fraud.

Furthermore, as can also be seen from our earlier submission, the screening services which we offer (e.g., OLS, BNS) are only as good as the IXC/Operator Service Provider's ("OSP") interest in finding out whether they have been asked for by an individual customer.[83] Thus, barring a mandate that they be checked by all IXCs/OSPs, such offerings are no more than aids to customers seeking to prevent fraudulent conduct.

Even if the Commission did mandate carrier queries with regard to LEC screening services, however, it would not necessarily mean that the LECs' networks (or their databases)

---

[83]See U S WEST at 19-20, 22-23. Compare IPANY at 11 (where it suggests that LECs' failure to design a "system which assures that screening digits . . . is [sic] passed through to all IXCs and all IXC operators, in all calling scenarios, constitutes negligent or irresponsible management for which LECs should and must be held accountable." U S WEST is unclear what is meant by this assertion. Certain screening services do transmit information on all calls (e.g., OLS) but not all IXCs/OSPs have the system capability or interest (apparently) to "translate" the information. See U S WEST at 19-20, 22-23. This can hardly be defined as a LEC management problem. Other restricted called party information is available through a LIDB inquiry (e.g., BNS). The failure of an IXC/OSP to query LIDB also cannot be declared as an act of "LEC" negligence. Indeed, the Commission would declare either scenario (we suspect) as a failure of an IXC/OSP to "do [its] part" in the area of fraud prevention. See In the Matter of Local Exchange Carrier Line Information Database, Order, 8 FCC Rcd. 7130, 7135 ¶ 33 (1993). Thus, IPANY's conclusion that "[T]he only likely reason for failure [of BNS screening] is the LEC's failure to correctly enter the data[,]" is simply incorrect. IPANY at 11. It does, however, demonstrate the lack of analyses generally represented by those commentors urging greater LEC liability in the matter of payphone toll fraud.

would be the best place to house/secure information associated with such new offerings. U S WEST doubts whether, at this time, anyone really knows. A decision on this matter would undoubtedly involve serious consideration of the impending intelligent networks and burgeoning network/adjunct providers, as well as the appropriate synergy between the IXC and LEC network elements.[84] It is simply not a determination that can be made based on the existing record.

For this reason, U S WEST encourages the Commission to refrain from mandating that LECs create any additional network monitoring or blocking/screening services, at this time. As Sprint suggests it is important to both know and analyze the placement of various services so that inappropriate redundant services/capabilities are not created in the various constituent networks.[85] This is precisely the kind of issue that should be reviewed by an expert organization, such as the TFPC, with the benefit of full industry and customer participation.[86] U S WEST encourages the Commission, should it remain interested in this matter, to refer the issue to just such an organization.

---

[84]Compare Sprint at 16, 19.

[85]See id.

[86]See further discussion below at Section VI.

III. EXISTING LEC LIMITATIONS OF LIABILITY ARE NOT UNLAWFUL OR CONTRARY TO PUBLIC POLICY -- FURTHERMORE, WHILE INSULATING LECS FROM FRAUD LIABILITY ABSENT GROSS NEGLIGENCE, THEY DO NOT REFLECT AN INAPPROPRIATE ALLOCATION OF THE RISKS OF FRAUD

A. Limitations of Liability

As NYNEX and PRTC/PRCC correctly argue, carrier limitations of liability have been upheld repeatedly by both this Commission and the courts as representing reasonable tariff provisions.[87] They are economically and commercially sound, as a general matter. But more particularly with regard to the matter of fraud, they represent an appropriate alignment between control and responsibility.

As certain commentors contend, telecommunications fraud has become increasing a customer problem as the intelligence formerly lodged securely in the network has migrated to the CPE accessing that network.[88] It would be inappropriate, from both technological and public policy perspectives to either ignore this migration or pretend the Genie can be put back in the bottle. Customers must be responsible for choices they make, ranging from what businesses to be in to what CPE to buy in support of those business enterprises. Customers must learn how to manage the intelligence they purchase, or they should not purchase it in the first instance.

---

[87] See NYNEX at 10-15; PRTC/PRCC at 3-5.

[88] See, e.g., GTE at 2; AT&T at 10 n.9; TFS at 4; WilTel at 2, 9 (all citing to NPRM ¶ 3).

Thus, from a liability assessment perspective, it would send totally inappropriate signals to customers for the Commission to relieve them of liability caused by the interaction of their CPE with the foundational public network. There is not, currently, any "imbalance in allocation of liability between carriers" and customers.[89] The balance is legitimate and appropriate: First and foremost, liability should remain with the customer.[90]

Aside from the philosophical and economic soundness of assigning primary responsibility for fraud occurrences to the CPE owner, there is the additional problem of attempting to fashion what others might claim to be a more "equitable" approach. Various possibilities exist. One possibility is that a customer (CPE owner) is liable only for negligence,[91] whereas all non-negligent customer fraud costs are borne by either network providers or manufacturers/suppliers. This could easily result in situations where a network provider or a manufacturer/supplier would be liable for fraud regardless of any responsibility or

---

[89]APCC at 4.

[90]Where liability is appropriately lodged and assigned to the customer, a carrier's limitation of liability really plays no part. It is only when the customer complains about the assignment that the matter is fairly easily dismissed by a discussion of liability assignment and a reference to the tariff limitation.

[91]This seems to be the overwhelming position of most CPE-owner commentors, although (as noted in nn.33-35 supra) the basic position has a couple of variations.

control over the device(s) that permitted the fraud to occur,[92] as well as for the provider's own simple mistakes.[93] Under this model, a CPE owner would not be held responsible when it made a "mistake," the carrier or the supplier would be, and the carrier/supplier would always be responsible for its own

---

[92]This could be true where the customer made a "mistake" short of negligence. This seems to be what Stop & Shop alleges occurred with regard to at least two instances of fraud affecting it ("an error occurred during the performance of routine maintenance activities that changed or left access to our outbound services unrestricted."). Stop & Shop at Attachment B, 1. See id. at 3. But see CompTel at 4; AT&T at 11; MCI at 3, 5, 7 (all correctly asserting that total control over the telecommunications system resides with the CPE owner and that the carrier lacks any capability to control the CPE or engage in risk protection activity with respect to it).

[93]Generally, an entity making a mistake is not even deemed to have acted unreasonably under the law, i.e., a mistake does not equate with negligence.

mistakes.[94] This would be a radical departure from existing carrier liability principles.[95]

Currently, CPE owners are liable for not just their negligence but for their mistakes. The Commission should not change that responsibility because it is the CPE owner -- not the carrier -- which is best positioned to protect against mistakes. Thus, the Commission should reject any liability theory that holds CPE owners liable only for negligence.

Another possible model is that a CPE owner is responsible absent carrier/supplier negligence. This would provide certain basic protections to carriers/suppliers in the event of

---

[94]There are commentors in this docket that urge liability on carriers for "mistakes," thus rendering the carrier strictly liable. See, e.g., IPANY at 10 (LECs should be liable for fraud resulting from LEC errors, such as failing to properly enter and execute blocking/screening service orders; failing to transmit screening codes to IXCs or failing to enter restricted line information into BNS databases. Ignoring all human capacity for error, IPANY asserts that "[a]bsolutely no excuse for such failure exists." Id. Of course, it does: human error short of negligence. Compare id. at 22). See also FPTA at 5 ("Sometimes the OLS or BNS information is either not delivered by the LEC . . . to its operator position or otherwise overlooked or ignored by the operator."), 11 ("sometimes [services] fail[] to work"); NJPA at 2 (LECs should be responsible for "the failure of screening processes").

One has to question has much fraud is caused by LEC errors, short of negligence. Perhaps a "prime causes" of fraud schematic could be helpful in working through fault allocations. A LEC error would, certainly, be near the bottom of the list.

[95]See NYNEX at 11. While certain carriers express a willingness to assume such responsibility (see BellSouth at 6-7; but see id. at 13 where BellSouth indicates that its liability should depend on the absence of reasonable care, i.e., negligence), U S WEST cannot imagine the adoption of such a model barring a demonstration that such was compelled by the public interest. We believe no such demonstration has been made.

"mistakes," but would render them responsible for what the law would deem "unreasonable" conduct.[96] This too would be a significant and material departure from existing carrier liability principles.[97] And, it would require -- in each instance -- a factual forum in which the matter of "reasonableness" was determined.[98] This would be costly to all parties involved, particularly to the carriers (as it could be expected that in each and every instance carrier negligence would be asserted). It would not be a prudent exercise of legislative prerogative regarding risk and liability allocations to establish such a liability model for one class of customer with one type of injury.[99]

---

[96]While the Commission has certain controls over manufacturers and suppliers via its Part 68 registration rules, it is not clear that the Commission should promulgate an enforceable rule with regard to manufacturer/supplier negligence, absent some revision of the Communications Act. A manufacturer/supplier will remain free, after this proceeding, to limit liability or limit its warranties through its private contractual relationships with purchasers. Compare User Parties at 4. The Commission would undoubtedly be exceeding its Part 68 authority if it were to try to prevent such contractual provisions by refusing equipment registration if such provisions were used. The end result of this phenomenon would be that manufacturers/suppliers could continue to limit their liability for fraud, or specify particular remedial measures for their mistakes/negligence, but that carriers could not. Thus, residual fraud liability would remain, and the question would continue: who should bear the costs associated with this residual liability? Clearly, it would not be appropriately allocated to network providers.

[97]To the extent that a carrier wanted to assume such responsibility, they obviously would be free to do so.

[98]See discussion below on "Comparative Fault."

[99]See U S WEST at 31-32.

Still another model is provided by Vanguard: "the costs of fraud [should be] based on whether a party had taken all reasonable steps to detect and prevent fraud[.]"[100] While the model has something to be said for it, i.e., it is an all-around "best efforts" approach to fraud prevention/risk allocation, it is still a fact-gathering/resolving process, which has the potential of consuming considerable carrier and judicial resources. In each case, a determination would have to be made as to what "all reasonable steps" were and whether each respective entity had complied. This would involve, as Vanguard points out, not just a determination of the facts, but a further qualitative analysis of the cost/benefit decisions made by each entity.[101] Furthermore, it would still provide no "fair" allocation of fraud costs in those circumstances where all parties took all reasonable steps to prevent fraud and fraud still occurred.

Because it is not unconscionable (from either a legal or public policy perspective) for the carrier to limit its liability for "negligence," which carriers have generally done with regard to all their actions and all their customers, it makes no sense to change the existing liability model in these circumstances. While this, no doubt, produces certain hardships on individual customers, the prices of the products/services that the carriers have developed to aid customers in fraud prevention activities

---

[100]Vanguard at 7 (emphasis added).

[101]See Vanguard at 7 & n.4.

will only increase if the model is changed[102] -- producing, perhaps, a depression in demand for the products/services themselves,[103] a totally counterproductive result.

For all these reasons, encompassing as they do sound economic, commercial and public policy rationales, the Commission should not disturb existing LEC limitations of liability, as they pertain to either carrier/customer or carrier/carrier relationships.[104] The Commission can always reinvestigate this matter, if it believes that the continuation of such limitations produces disturbing unwarranted or unreasonable results.[105] But, at this time, such liability limitations have not been demonstrated to have produced aberrant market or unconscionable results. Such tariff provisions should be permitted to continue.

B. Comparative Fault Model

A number of parties urge the Commission to adopt a comparative fault model of fraud dispute resolution,[106] although

---

[102]See, e.g., NYNEX at 10; Rochester at 9.

[103]See, e.g., id.

[104]This latter relationship is discussed in more detail below, with regard to LIDB offerings.

[105]See Sprint at iii, 23.

[106]As the Joint Commentors correctly point out, carriers "existing tariff liability provisions are logically incompatible with a shared liability concept." Joint Commentors at 5 n.9. Thus, the Commission need only consider a comparative fault approach if it is determined to move away from the existing model.

not always using that precise term.[107] A review of those commentors' positions demonstrates the administrative burden associated with "fact-based" dispute resolution. In virtually every case there would be required a review of the facts, a comparison of those facts to either a general "reasonable" standard of behavior[108] or to a more "definitive" statement of roles/responsibilities as previously adopted by the Commission (or devised by some industry group).[109] Some even argue for a

---

[107]See, e.g., Ad Hoc at 3-4; API at 6-8; FMC at 2-3 (who cites to the "facts" of a case involving it, leaving one to wonder if the facts would not be recited very differently if proffered by the carrier); ICA at 9-10; Joint Commentors at 3, 6-8; McCaw at 13-14 (suggests that in certain circumstances LECs should bear a portion of toll fraud associated with cellular calls); NJPA at 1; Pinellas County at 5-6, 8 (reciting various facts that might make end users behave differently and recommending a fault resolution structure); RAK at 4-5 (citing the factual considerations to be considered in determining entity liability); TCA at 7-8; User Parties at 6; UTC at 4-7.

[108]Compare Joint Commentors at 6 ("The applicable duty would vary depending upon the parties' relationship to the toll fraud situation." Joint Commentors then provides certain "examples."); UTC at 4 ("In developing comparative negligence rules for toll fraud it is necessary to determine the responsibilities of the various parties." UTC then goes on, with some degree of specificity, to identify what "duties" it sees carriers as having, concluding with the observation that customers should "be obligated to employ reasonable measures" and to exercise "reasonable care to prevent unauthorized access to their system," with no delineation of specifics.) id. at 6; Ad Hoc at 3-4 ("Only if the carrier can show that the proximate cause of the loss was the negligence or willful misconduct of the customer -- and that the carrier did not have the 'last clear chance' to avoid or prevent the loss, such as by using reasonable network monitoring techniques -- should the loss fall on the customer.") (footnote omitted).

[109]A number of commentors supporting a comparative negligence model set out what they consider to be appropriate carrier "duties" and then describe how their model would play out. For example, User Parties states, "thus, if a carrier failed to

(continued...)

shift in the burden of persuasion from the complaining customer to the carrier.[110] As is obvious, the process would be costly

---

[109](...continued)
provide timely notice that a parameter had been exceeded, it would be liable for the resulting fraud losses. The carrier would also be liable if it failed to provide unrated call detail within the three-hour time period, or if it failed to respond in a timely manner to a customer's report of suspicious activity. Conversely, if a customer failed to take steps to mitigate unauthorized use after being notified of usage anomalies, the customer would be responsible for the loss. Similarly, if a customer declines to purchase fraud prevention services after being notified by the carrier of the risks of unauthorized usage, the customer should be liable for any unauthorized calls resulting from CPE-based fraud." User Parties at 6. User Parties concludes by stating that "in no circumstances . . . should a customer be held responsible for fraud losses resulting from a hacker's infiltration of the carrier's premises or equipment." Id. at n.12.

TCA, on the other hand, outlines certain "customer responsibilities," suggesting that if the customer complies "with the . . . requirements" the customer "will have discharged its obligation to minimize toll fraud." TCA at 8, listing six customer obligations. Obviously, each of these would have to be factually explored in a comparative negligence context.

API has one of the most detailed models of all. It would divide carrier/customer toll fraud responsibility into three separate Phases, with different responsibilities/duties (as well as time frames) assigned to each Phase. See API at 8-11. As a general matter, API leaves customers responsible for fraud "until such point as the carriers are reasonably capable of detecting such fraud" (id. at 7); then converts liability to the customer for 50% of the fraud (with additional responsibility attending for negligence. API outlines examples of customer negligence. (Id. at 11.); then after carrier notification/customer acknowledgement, responsibility lies with the customer. No serious analysis is given, however, to the fundamental issue that network monitoring is not well-suited to general fraud prevention (especially with regard to large businesses) (see discussion above at Section II.A.), and that discrete network lines/trunks that require monitoring for fraud should be specifically identified to carriers and then monitored for a charge. See earlier discussion at Section II.A.

[110]See UTC at 6 ("the carriers and vendors should have the burden of persuasion to demonstrate that the customer did not employ reasonable measures to prevent/detect the toll fraud.").

and time consuming, and would not generally benefit the overall carrier customer base.

U S WEST agrees with Pacific and CompTel that "[n]either carriers nor the Commission have resources" for a case-by-case comparative negligence approach to fraud liability.[111] "Any system of 'comparative' liability for [CPE-based] fraud would be an administrative and litigious nightmare by requiring ad hoc, case-by-case adjudication."[112]

Furthermore, a comparative "fault" model assumes some party was at fault. That is not necessarily the case, as is demonstrated by certain of the filed comments.[113] Much time and money could well be spent on an individual case adjudication, only to determine that no one was at fault. In such a circumstance, only some kind of arbitrary allocation of

---

[111]See Pacific at 12. Compare AT&T at 15-16 (stating that such a process would "focus upon the actual manner in which the fraud occurred and the actions of the party or parties who had control over the information, equipment or network element which allowed the fraud to occur."); Sprint at 9 ("Because the list of toll fraud scenarios could be enormous, any attempt to catalogue the specific conditions under which various parties are liable will be incomplete, will inevitably lead to disputes, and will embroil the Commission in a series of proceedings to determine the extent of each party's culpability.").

[112]CompTel at 3. Others objecting to a comparative fault model include Bell Atlantic at 5 n.5; Flex at 2; NYNEX at 16; Pacific at 12.

[113]See ISLUA passim; CompTel at 4; Sprint at ii, 9-10.

liability[114] would "resolve" the dispute. For all of these reasons, U S WEST agrees with CompTel in its following remarks:

> CompTel disagrees with the notion that liability can inevitably be assessed in individual cases on the basis of comparative fault or negligence. There is a broad continuum of measures which a [CPE] owner can take to prevent or minimize the likelihood of fraud. It is a business decision for each [CPE] owner to decide which measures are most appropriate in its own circumstances. That a [CPE] owner ultimately is a victim of toll fraud does not mean that the owner, or anyone else, made the wrong decision or was otherwise negligent or at fault. Like all insurance, [CPE] security is an exercise in probabilities rather than certainties. Because toll fraud may occur in circumstances where no party is to blame, it makes no sense to establish a system of comparative liability or to remove liability from the [CPE] owner who is responsible for making the decisions about how much and what kinds of toll fraud "insurance" it should obtain.[115]

For all of the above reasons, the Commission should eschew any comparative fault model for allocating fraud liability. It is simply unworkable and unnecessary. Individuals who believe that they have been outrageously treated with regard to telecommunications fraud have the complaint process available to them. While U S WEST cannot say it agrees with all of the Commission's decisions,[116] the process does provide those CPE

---

[114]Such as that which was proposed by H.R. 6066, 102d Congress, 2d Session, Sept. 30, 1992. Compare AT&T at 13; ISLUA at 2.

[115]CompTel at 4.

[116]For example, like Rochester, we disagree with the Commission's resolution of the United complaint. See Rochester at 8 n.16. Either United was a customer of AT&T's (as the fraud occurred through the utilization of AT&T's facilities) or it was a carrier in its own right.

owners/COCOT providers who believe they have been treated unfairly a forum to air their grievances. Nothing additional is required by way of either fairness or policy.

V. NEITHER LEC CALLING CARDS NOR LEC LIDBS "CAUSE" TELECOMMUNICATIONS FRAUD - NEITHER SHOULD BE BURDENED -- AS A MATTER OF REGULATORY FIAT -- WITH INCREASED FRAUD PREVENTION/DETECTION OR LIABILITY COSTS

Certain commentors, while contending that their houses are all in order with regard to customer relationships and fraud matters,[117] argue that LECs' calling cards have somehow created an environment conducive to fraud,[118] and yet LECs lack economic incentives to control the resulting fraud, i.e., that they have no economic incentive to produce a quality LIDB product.[119] U S WEST disagrees. U S WEST's current limitation of liability does not produce counter incentives to fraud prevention with regard to our calling cards or the LIDB, anymore than it does with regard to our end-user customers.

A. LECs' Calling Cards Allow for Increased Interexchange Calling (for which IXCs Secure Substantial Revenues) - IXCs are not Compelled to Accept (Honor) Such Cards, nor Does Their Existence Produce Uncontrollable Fraud Problems

TFS argues that the existence, and promotion, of LEC calling cards have created the necessity for IXCs to "accept" them, as

---

[117] See, e.g., AT&T at ii, 2; MCI passim; TFS at 5.

[118] See, e.g., TFS at 11-14.

[119] See AT&T at 2, 29, 32; MCI at 14; TFS at 5, n.2.